This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims

Claim 1 (Original): A method comprising:

minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of the stick, and a length of the stick;

spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and

depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset spent by the user from the stick and passing the vendor-signed composite along with the issuer-signed composite to the issuer.

Claim 2 (Original): A method as recited in claim 1, further comprising storing the stick of electronic assets in a tamper-resistant electronic wallet.

Claim 3 (Original): A method as recited in claim 1, further comprising storing the stick of electronic assets in an electronic wallet constructed with a secure-processor architecture.

Claim 4 (Original): A method as recited in claim 1, wherein the minting comprises minting the stick of assets using a blind signature protocol.

Claim 5 (Original): A method as recited in claim 1, wherein the spending comprises:

concatenating a vendor identity with the first asset from the stick to form a payment request;

signing the payment request with a signature of the user:

submitting the user-signed payment request along with the issuer-signed withdrawal request to the vendor;

accepting the first asset as payment in an event that the user and the issuer are verified; and

subsequently passing any additional assets from the stick as payment to the vendor without digitally signing them with the user's signature;

Claim 6 (Original): A method comprising:

minting a stick of electronic assets by digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of the stick, and a length of the stick;

spending one or more assets from the stick at one or more vendors, wherein each expenditure with a particular vendor involves digitally signing with a user's

signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the particular vendor for verification and subsequently passing any additional assets to be spent without user signature to the particular vendor; and

depositing one or more assets collected by the particular vendor by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset spent by the user from the stick and passing the vendor-signed composite along with the issuer-signed composite to the issuer, wherein the depositing comprises:

concatenating the user-signed first asset $S_U(Cj)$, a last asset spent from the stick *Ck*, and a run length *RL* of assets beginning with the first asset *Cj* and ending with the last asset *Ck* to form a deposit request;

signing the deposit request with a signature of the vendor:

$$S_V(S_U(Cj), Ck, RL)$$

submitting the vendor-signed deposit request along with the issuer-signed withdrawal request to the issuer; and

crediting a vendor account with the run of assets in an event that the user, the vendor, the run, and the issuer are positively verified.

Claim 7 (Original): A method as recited in claim 1, further comprising auditing the assets deposited by the vendor.

Claim 8 (Original): A method as recited in claim 1, further comprising auditing a sample of the assets paid by the user to the vendor.

Claim 9 (Original): A method as recited in claim 1, further comprising selecting, at the vendor, a subset of less than all of the assets paid by the user to the vendor and submitting the subset of assets to an auditor for fraud evaluation.

Claim 10 (Original): Distributed computer-readable media resident at the issuer, user, and vendor having computer-executable instructions to perform the method as recited in claim 1.

Claim 11 (Original): Computers resident at the issuer, user, and vendor that are programmed to perform the method as recited in claim 1.

Claim 12 (Original): A method for issuing electronic assets, comprising:

forming a stick of L electronic assets C_i (for i=1, ..., L) where each asset can be derived from a preceding asset in the stick;

signing the stick with a signature of a party issuing the assets;

spending a first run of one or more assets from the stick at a first vendor; and

spending a second run of one or more assets from the stick at a second vendor.

Claim 13 (Original): A method as recited in claim 12, further comprising storing the stick of electronic assets in a tamper-resistant electronic wallet.

Claim 14 (Original): A method as recited in claim 12, further comprising storing the stick of electronic assets in an electronic wallet constructed with a secure-processor architecture.

Claim 15 (Original): A method as recited in claim 12, wherein the forming comprises anonymously issuing the stick of assets using a blind signature protocol.

Claim 16 (Original): A method as recited in claim 12, wherein the forming comprises:

creating the stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a one-way hashing function of a value x.

Claim 17 (previously amended): A method for issuing electronic assets, comprising:

forming a stick of L electronic assets C_i (for $i=1, \ldots, L$) where each asset can be derived from a preceding asset in the stick; wherein the forming comprises:

creating the stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a one-way hashing function of a value x;

constructing a withdrawal request having a user identity U, a user secret K, a last asset value C_L taken from a bottom of the stick, a denomination d indicating a value for the assets in the stick, an expiration t, and the value L; and

signing the withdrawal request with a signature of an issuer:

$$S_I(U, K, d, C_L, t, L);$$

signing the stick with a signature of a party issuing the assets;

spending a first run of one or more assets from the stick at a first vendor; and

spending a second run of one or more assets from the stick at a second vendor.

Claim 18 (Original): A method as recited in claim 12, wherein the spending comprises:

signing a first asset from the stick with a signature of the user:

submitting the user-signed asset along with the signed stick to the first vendor; and

in an event the first asset is accepted, subsequently submitting any additional assets from the stick without digitally signing them.

Claim 19 (Original): A method as recited in claim 12, further comprising auditing the assets from the first and second runs of assets for fraud.

Claim 20 (Original): A method as recited in claim 12, further comprising auditing a sample of assets from the first and second runs of assets for fraud.

Claim 21 (Original): A method as recited in claim 12, further comprising depositing the first and second runs of assets.

Claim 22 (Original): Computer-readable media resident at the issuer and the user having computer-executable instructions to perform the method as recited in claim 12.

Claim 23 (Original): Computers resident at the issuer and the user that are programmed to perform the method as recited in claim 12.

Claim 24 (Original): A method for issuing electronic assets, comprising:

creating, at a user, a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

submitting a withdrawal request from the user to an issuer, the withdrawal request having a user identity U, a last asset value C_L taken from a bottom of the stick, and the value L, while omitting any vendor identity;

signing, at the issuer, the withdrawal request; and

returning the signed withdrawal request to the user.

Claim 25 (Original): A method as recited in claim 24, further comprising storing the stick of electronic assets and signed withdrawal request in a tamper-resistant electronic wallet.

Claim 26 (Original): A method as recited in claim 24, further comprising storing the stick of electronic assets and signed withdrawal request in an electronic wallet constructed with a secure-processor architecture.

Claim 27 (Original): A method as recited in claim 24, wherein the withdrawal request further has a user secret *K*, a denomination *d* indicating a value for the assets in the stick, and an expiration *t*.

Claim 28 (Original): A computer-readable medium having computer-executable instructions that direct an electronic wallet to perform the method as recited in claim 24.

Claim 29 (Original): A computer programmed to perform the method as recited in claim 24.

Claim 30 (Original): A computer-readable medium storing the stick of electronic coins and the signed withdrawal request constructed as a result of the method as recited in claim 24.

Claim 31 (Original): A method comprising:

creating, at a user, a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

submitting a withdrawal request from the user to an issuer, the withdrawal request having a user identity U, a user secret K, a last asset value C_L taken from a bottom of the stick, a denomination d indicating a value for the assets in the stick, an expiration t, and the value L;

signing, at the issuer, the withdrawal request:

$$S_I(U, K, d, C_L, t, L)$$

returning the issuer-signed withdrawal request to the user;

initiating payment of one or more assets from the stick to a vendor having an identity V;

concatenating, at the user, the vendor identity with a first asset Cj to be spent from the stick to form a payment request, and a depth D indicating a distance of the first asset from the bottom of the stick;

signing the payment request with a signature of the user:

$S_U(Cj, D, V1)$

submitting the user-signed payment request along with the issuer-signed withdrawal request to the vendor;

accepting the first asset as payment at the vendor in an event that the user and the issuer are verified;

subsequently passing any additional assets from the stick as payment to the vendor without digitally signing them with the user's signature;

concatenating, at the vendor, the user-signed first asset, a last asset spent from the stick *Ck*, and a run length *RL* of assets beginning with the first asset *Cj* and ending with the last asset *Ck* to form a deposit request;

signing the deposit request with a signature of the vendor:

$S_V(S_U(Cj), Ck, RL)$

submitting the vendor-signed deposit request along with the issuer-signed withdrawal request to the issuer; and

crediting a vendor account with the run of assets in an event that the user, the vendor, and the issuer are verified.

Claim 32 (Original): A method as recited in claim 31, further comprising randomly selecting an asset from the assets paid by the user to the vendor and submitting the selected asset for audit.

Claim 33 (Original): A method as recited in claim 31, further comprising auditing the assets deposited by the vendor with the issuer.

Claim 34 (Original): A method for anonymously issuing electronic assets, comprising:

creating, at a user, a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

blinding the stick using a random value p, where:

$$\text{Blind Stick} = p^e C_L \bmod N$$

where C_L is a bottom asset on the stick;

submitting a withdrawal request from the user to an issuer, the withdrawal request having the blind stick and the value L;

signing, at the issuer, the withdrawal request by computing:

$$c = (p^e C_L)^{Lf} = p^L C_L^{Lf} \bmod N$$

where e and f are public and private variables known by the issuer and e is known to everyone;

returning the signed withdrawal request to the user;

deriving a new bottom asset by computing:

$$C_L^{Lf}=c/p^L \bmod N.$$

Claim 35 (Original): A method as recited in claim 34, further comprising storing the blind stick of electronic assets and signed withdrawal request in a tamper-resistant electronic wallet.

Claim 36 (Original): A method as recited in claim 34, further comprising verifying the bottom asset by computing C_L^{Lf} independently and comparing a result to the new bottom asset derived in said deriving (C_L^{Lf})

Claim 37 (Original): A method as recited in claim 34, further comprising storing the blind stick of electronic assets and signed withdrawal request in an electronic wallet constructed with a secure-processor architecture.

Claim 38 (Original): A method as recited in claim 34, further comprising spending an asset from the blind stick by first sending the new bottom to a vendor for verification.

Claim 39 (Original): A computer-readable medium having computer-executable instructions that direct an electronic wallet to perform the method as recited in claim 34.

Claim 40 (Original): A computer programmed to perform the method as recited in claim 34.

Blank

Claim 41 (Original): A computer-readable medium storing the blind stick of electronic coins and the signed withdrawal request constructed as a result of the method as recited in claim 34.

Claims 42-50 (Withdrawn)

42 Claim ~~51~~ (Original): An electronic asset system comprising:

an issuer wallet having a processor and storage, the issuer wallet digitally signing with an issuer's signature a composite of user-provided data items including a user identity, a bottom asset from a bottom of a stick of electronic assets, and a length of the stick;

52

a user wallet having a processor and storage to store the stick of electronic assets and issuer-signed composite and to spend one or more assets from the stick at one or more vendors, the user wallet spending one or more assets by digitally signing with a user's signature a first asset from the stick to be spent and passing the user-signed first asset along with the issuer-signed composite to the vendor for verification; whereupon verification, the user wallet subsequently passes any additional assets to be spent without user signature to the vendor; and

a vendor wallet having a processor and storage to store one or more assets spent by the user wallet, the vendor wallet depositing the assets collected from the user wallet by digitally signing with the particular vendor's signature a composite of data items including the user-signed first asset and a last asset passed in the

stick received from the user wallet and passing the vendor-signed composite along with the issuer-signed composite to the issuer wallet for verification.

Claim 43 (Original): An electronic asset system as recited in claim 42, wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-resistant.

Claim 44 (Original): An electronic asset system as recited in claim 42, wherein the issuer wallet, the user wallet, and the vendor wallet are tamper-resistant constructed with a secure-processor architecture.

Claim 45 (Original): An electronic asset system as recited in claim 42, wherein the issuer wallet signs the composite using a blind signature protocol.

Claim 46 (Original): An electronic asset system as recited in claim 42, further comprising an auditing system to audit the electronic assets to detect whether assets have been used in a fraudulent manner.

Claim 47 (Original): An electronic asset system as recited in claim 42, further comprising a probabilistic auditing system to sample a subset of less than all electronic assets to detect whether assets have been used in a fraudulent manner.

Claim ~~57~~ 46 (Original): An electronic wallet having memory and a processor, the electronic wallet being programmed to:

create a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

form a withdrawal request having a user identity U, a last asset value C_L taken from a bottom of the stick, and the value L, while omitting any vendor identity;

submit withdrawal request to an issuer and receive the withdrawal request back with an issuer signature; and

store the signed withdrawal request and the stick.

Claim ~~58~~ 47 (Original): An electronic wallet having memory and a processor, the electronic wallet being programmed to:

create a stick of L electronic assets by computing:

$$C_i = h^i(x) \quad (\text{for } i=1, \ldots, L)$$

where $h(x)$ is a hashing function of a value x;

form a withdrawal request having a user identity U, a last asset value C_L taken from a bottom of the stick, and the value L, while omitting any vendor identity;

submit withdrawal request to an issuer and receive the withdrawal request back with an issuer signature;

store the signed withdrawal request and the stick;

form a payment request for payment of one or more assets from the stick to a vendor having an identity *V*, the payment request having the vendor identity *V* and a first asset *Cj* to be spent from the stick;

sign the payment request:

$$S_U(Cj, V1);$$ and

submit the signed payment request along with the signed withdrawal request to the vendor.

Claims 59-60 (Canceled).